

Fast, Cheap and Out of Control - Internet/Web/Online Service Information

Stewart Taggart

As long as there have been borders, people have crossed them in search of the most advantageous legal environment. It's called regulatory arbitrage, and the Net is now making it easier than ever.

Care to bank from a Pacific Island, store your online data in Scandinavia and pay taxes in Barbados? A nicer mix of financial secrecy, data privacy and low government levies would be hard to imagine.

If this multijurisdictional legerdemain appeals to you, James Bennett could be your man. He's in the business of providing, as he calls them, "sovereignty services." For a fee, he'll slice and dice your business or personal affairs to put them in the best mix of global jurisdictions to keep the authorities off your back.

"Anguilla has nice privacy laws and low taxes, but they've had some scams over there," Bennett says. "Meanwhile, Scandinavian countries aren't financial tax havens, but they do have very strong data privacy laws and good courts. It depends on what you're after."

Bennett, who has been mixed up in everything from commercial rocketry as president of American Rocket Company to nanotech research as director of the Foresight Institute, founded Internet Transactions Transnational in 1997. He expects his Virginia-based company to be up and running by the end of this year. Initially the company will focus on arranging the affairs of wealthy individuals, but Bennett plans to branch out later into business services, using virtual private networks, proprietary authentication and arbitration methods and a system of global access points.

"The nice thing about the Internet is that it allows you to link -- cheaply -- a number of jurisdictions with different characteristics," he says. "We just aim to lower the threshold cost."

Like others, Bennett is an entrepreneur looking to make an Internet buck off of one of our oldest activities: regulatory arbitrage.

Simply put, regulatory arbitrage involves exploiting differing rules in different jurisdictions - for a profit. Think back to when you were a kid. If Mom wouldn't give you a dollar, you asked Dad for one. If they both said no, you asked your aunts and uncles when they visited. The system works in childhood so we use it throughout our lives.

Salesmen seek out the easy marks among buyers in an organization, physicists look for paths of least resistance in experiments and lawyers readily engage in jurisdiction shopping for sympathetic courts. Shipping companies operate under flags of convenience, Switzerland and Liechtenstein profit from discrete domestic banking secrecy laws and multinationals adroitly shift manufacturing to places where safety laws are lenient.

Now entrepreneurial dot-coms are trying their hand at the game. To an arbitrageur, regulations are a price that businesses, consumers of jurisdictional services, pay. Just as the Internet has brutally exposed global product-pricing inefficiencies, the Net's now being used to assault the leather-bound world of national regulations. The enabler here is the near-frictionless ability the Internet provides to shift data-based businesses across fiber cables in search of the friendliest home.

"The sovereignty question is one of the most interesting frontiers in cyberspace," says Bennett. He should know. While his company, IITI, is physically based in northern Virginia, it is incorporated in the Bahamas and operates primarily out of Ireland.

But the way IITI is set up is merely one way to shuffle the deck, Bennett says. With more than 200 global jurisdictions to choose from, and the ability to relocate a business at the speed of a mouse click, the process of building new global business architectures from the modem up is just getting started.

Overtime, all this border-hopping may lead to a showdown between entrepreneurs and the forces of control at the local, domestic and international levels. But it's an open issue whether more than 200 governments can clamp down without sacrificing beneficial business experimentation.

Most experts agree on one point: Within today's increasingly open electronic borders, the possibilities look pretty limitless - at least for the little guy and at least for the short-term. In the words of one lawyer familiar with the issue: "It's pretty hard to arrest an electron."

WAGES OF CONFUSION

Most people have heard about the benefits of regulatory arbitrage -- and the horror stories -- even if they don't know its name. For every Chinese dissident spreading his views freely from the haven of a Silicon Valley Internet server, there's a would-be gangster, money launderer or pedophile plying his trade from an indifferent island, steppe or anarchic political entity. It is the middle ground, however, where the real opportunists are staking their turf. For the likes of Vincent Cate and others, global regulatory muddles spell one thing: money.

From sunny Anguilla, a British dependency, Cate runs a Web site (www.publicdata.com.ai) that provides access to various U.S. records. Many of these are mundane things like drivers' license data, but Cate's site also publishes hotter items like voter rolls and even criminal files. Some of these records are prohibited in the U.S. from being put online. Texas, for example, sells drivers' license records, but only on the condition that they not be posted on the Web, says Cate.

Cate, though, operates from the Caribbean, where drug runners and sunburns are bigger concerns than Texas state troopers. Lone Star State privacy rules? Who cares. Anguilla's laws govern him. And the island has few recognizable statutes regarding disclosure of personal data, he says.

Cate won't say how he gets his Texas records, but he insists his methods are legal. If Texas should get wise and turn off his data spigot, he's confident he'll find another way to gather data. Like Bennett, Cate doesn't think he's doing anything wrong. He's just profiting from global data market inefficiencies and regulatory incoherence. Privacy issues represent a classic example of these discrepancies, he says.

"On the one hand, in the U.S. things like the Freedom of Information Act specify information must be given out, but on the other hand, privacy laws specify information must be kept secret," he says.

It's conflicts like these that keep him in business, and he sees little reason to get into another line of work. "I've been at this for three years now," he says. "So far, no state has ever tried to contact me."

Other opportunities exist elsewhere. Take gambling.

Proposals to ban many forms of online gambling have worked their way through the U.S. Congress. The most recent attempt was rejected by the House of Representatives July 18. In the wake of ongoing U.S. regulatory uncertainty, several gambling sites have instead set up shop in the Caribbean, even though it has yet to be proven whether local authorities can provide a workable legal framework for protecting consumers there.

Two years ago, Australia stepped into this niche. As a mature industrial democracy, Australia reckoned it could offer credibly regulated online gaming. Australia would draw a competitive advantage from a kind of arbitrage in reverse: Online bettors -- confident in Australia's regulation -- would be drawn to Australian online casinos.

New York-based General Media Communications, parent company of Penthouse, lined up for a license in Australia. Ironically, though, while Australia has more liberal online gambling regulations than the United States, it has stricter laws regarding the distribution of sexually explicit material over the Internet.

If General Media gains an Australian Internet gambling license, it will enjoy the best of both jurisdictions: U.S. laws applying to its online distribution of sexually explicit material and Australian laws applying to its online gaming operations. It's hard to imagine a neater illustration of regulatory arbitrage.

RULE OF LAW

Where regulatory arbitrage creates competitive advantage, entrepreneurs will rush in. The Internet is rapidly increasing such opportunities. If evanescent dot-coms can now largely pick and choose among more than 200 global jurisdictions in the near-frictionless mobility of the Internet age, can any one nation's regulatory regime survive?

Yes, says Michael Froomkin, a professor of law at the University of Miami and an expert in regulatory arbitrage. How? By following it the money.

At the root of regulatory arbitrage is profit. The currency of profit is money. And the warehouse for money is banks. As long as choke points like banks govern the flow of global finance, profits from regulatory arbitrage can be regulated, Froomkin argues. And as profits go, so goes the rest of a business.

Specifically, Froomkin says, governments can hit alleged miscreants where it hurts most: tax havens.

In late June, the Paris-based Organization for Economic Cooperation and Development released a report naming 35 tax havens worldwide, including the likes of Liberia, Panama and the U.S. Virgin Islands. It recommends the worst of these either agree within one year to reduce "harmful tax practices" by 2005 and increase regulatory cooperation with other jurisdictions or face a progressive disconnection from the international financial system.

To Froomkin, this represents a powerful threat. Faced with financial ostracization -- for example, collective denial of foreign aid -- lenient governments can be bludgeoned into accepting global norms.

But what happens if even these financial choke points lose their effectiveness, for instance when "e-cash" starts circulating? Some forms of e-cash -- being little more than computer code -- spend more time on computers than they do in the banking system. As such, they might increasingly be exchanged directly between parties instead of cleared like a check through a bank.

The current financial system works well in coping with sheepish depositors carrying suitcases full of cash, but not so well with methods of exchange that fall completely outside the banking system. This worries Froomkin, who says that many governments may solve that problem by moving toward that ultimate police roadblock and binary strip search -- opening transiting packets to view what's inside.

"On the outside, it's hard to tell if an encrypted packet is money, speech or advice about a sexual problem," Froomkin says. "With e-cash, investigators will have to get inside and look at the packets themselves to determine if a money transfer is taking place."

"If things get to this level, it would represent a whole new order of intrusive supervision of global communications," he says. "It's this step that really worries me."

That's far too harsh, says sovereignty-seeker Bennett. Sure, governments may try to monitor global data traffic. The FBI's proposed national e-mail tapping "Carnivore" system, and the long-existent global spy network "Echelon" -- Carnivore's international counterpart -- are examples of this. Both are believed capable of searching huge amounts of data traffic for keywords or to track individuals.

But Bennett says encrypted communications and virtual private networking will offer increasingly strong defenses against such systems, since both can shield data traffic on the public network from prying eyes. These protections will cost money, limiting their widespread adoption. The result: another digital divide.

"This could lead to a society in which people willing to pay have more privacy than ever before in history," Bennett says. "Meanwhile, other people could end up with less privacy than ever before in history."

Bennett says aggressive action by governments against regulatory arbitrage could backfire. Under this scenario, arbitrageurs might simply opt out of traditional currencies and transactions. For instance, surreptitious business and personal debts might be paid by digitally exchanging rights to precious metal. Web companies like E-gold are already making this possible. It offers transaction services between counterparties denominated in gold, silver, platinum or palladium reserves held by a third-party custodian. E-gold transactions merely transfer rights to the physically held, underlying precious-metal reserves -- bypassing currencies like dollars altogether.

Bennett adds that, in any case, OECD member nations have a limited incentive to financially isolate tax havens. Big countries eventually will need these small nations' cooperation in fighting global threats like terrorism, bio-warfare or even computer viruses. The price of this cooperation may well be a willingness to look the other way regarding a few margarita-drinking tax cheats.

Cate, Anguilla-based data merchant and margarita-drinker, agrees. He says small countries will always have strong incentives to profit from rules that differ from norms of larger countries. Indeed, those differences may be just about all they have to sell. Like Bennett, he believes ostracizing arbitrage-friendly minnows may backfire. Bad publicity might even be good. "It could actually bring them business," Cate says.

And he agrees encrypted transfers, virtual private networks and any number of other evasive techniques provide powerful defensive tools.

"On the Internet, money can move between 100 jurisdictions in a morning," he says. "The idea of cutting off tax havens is just not going to work."

While the loss of supervisory control over the movement of online businesses may look threatening, it's unlikely to cause enough regulatory entropy to force the world into chaos, Bennett says. For individuals and businesses, other variables besides regulatory arbitrage rapidly come into play. These are things like credibility and trust, often termed broadly as sovereign risk. Would you want to put your servers and financial assets in Iraq, for example, even if the tax rate was zero?

"We avoid encouraging people to transact business in places where you can't have confidence in the judicial system," Bennett says. "One of the things we look for is the strength of the rule of law."

WHAT'S A NATION TO DO?

Ultimately, the issue boils down to what kind of global regulatory system we want: Should a nation attempt to extend its laws throughout cyberspace, since virtually every place in cyberspace is "local"? Should it yield its sovereignty to a set of international rules that could take years to negotiate? Or should it engage in some kind of selective enforcement?

A legal free-for-all in which every country unilaterally extends its domestic laws into cyberspace is clearly unworkable. With more than 200 global jurisdictions to satisfy, no dot-com could do business through a single Web site. But even building 200 Web sites individually tailored to the requirements of each jurisdiction wouldn't avoid the problem, since there's no way (as of yet) to prevent a particular Web site from being accessed from a particular jurisdiction.

A second alternative is to assign or create a treaty-based global organization to carry the cudgel of harmonization. But it could take years to agree upon the size and composition of such a body. Its deliberations would be achingly slow by Internet-time standards. The United Nations Convention on the Law of the Sea, for example, which governs a host of political, economic, technological and scientific issues on the open oceans, took 150 nations more than 14 years to negotiate before being signed in 1982. The agreement took another 14 years to go into effect.

A more nuanced approach is that of the International Organization of Securities Commissions, an informal grouping of securities and futures market regulators, including everyone from the U.S. Securities and Exchange Commission to the Ugandan Capital Markets Authority. They've banded together to align international rules among member states, sidestepping the usual sluggish diplomatic process by utilizing their own bureaucratic power.

In the area of securities law, for instance, they've agreed that enforcement measures over securities dealing should be determined in part by the level of "targeting" a given Web securities business engages in toward a particular jurisdiction.

If an Australian, say, goes out of his way to find a French Web site to buy financial securities that aren't or can't legally be sold in Australia, they've agreed to largely let that pass. But if a French Web site specifically targets large numbers of Australian investors in the securities prohibited for distribution in Australia, say by advertising in an Australian newspaper or putting the site in the .au domain, it could be deemed to fall within Australian regulatory dictates. The French regulatory bureaucracy, however, would do the dirty work of sanctioning the site. Agree bilaterally, enforce locally.

Close cooperation among global securities regulators, however, is possible only because they share an interest in enhancing efficiently functioning markets and safeguarding against global financial meltdown. This kind of urgency might not carry over so easily into other areas. Taxation, for instance, pits the interests of one nation against those of another. Your gain is my loss.

Some argue that loss of national control is inevitable, and that the Internet should be left to its own devices. Individuals will pick and choose from a menu of regulatory environments much as pedestrians do and choose the city streets they walk down based upon how safe or efficient they're considered. Believers in a "self-ordering" system say sites providing credible protection against fraud and abuse would naturally gain traffic due to their reputations.

In such a self-ordering world, branding would largely take the place of black-letter laws, indeed of sovereignty itself, and Internet traffic itself would become a real-time voting machine.

Under the power of a million mouses, might the nation-state eventually whither away -- stripped of power and its control of the barn door? That seems unlikely. For the foreseeable future, nations will continue doing their best to keep a hand in the game.

And so, too, will entrepreneurs like Bennett and Cate.

Stewart Taggart (staggart@nsw.bigpond.net.au) is a writer in Sydney, Australia.

COPYRIGHT 2000 Standard Media International

COPYRIGHT 2000 Gale Group